JOURNAL OF COMBINATORIAL THEORY, Series A 29, 142–150 (1980)

Resolvable Perfect Cyclic Designs

F. E. BENNETT, E. MENDELSOHN, AND N. S. MENDELSOHN

Department of Mathematics, The University of Manitoba, Winnépeq, Canada

Communicated by the Managing Editors

Received May 18, 1978

Let k, λ, and v be positive integers. A perfect cyclic design in the class PD(v, k, λ) consists of a pair (Q, B) where Q is a set with $|Q| = v$ and B is a collection of cyclically ordered k-subsets of Q such that every ordered pair of elements of Q are t apart in exactly λ of the blocks for $t = 1, 2, 3, \ldots, k-1$. To clarify matters the block $[a_1, a_2, \ldots, a_k]$ has cyclic order $a_1 < a_2 < a_3 \cdots < a_k < a_1$ and a_i and a_{i+t} are said to be t apart in the block where $i + t$ is taken mod k. In this paper we are interested only in the cases where $\lambda = 1$ and $v \equiv 1 \bmod k$. Such a design has $v(v-1)/k$ blocks. If the blocks can be partitioned into v sets containing $(v-1)/k$ pairwise disjoint blocks the design is said to be resolvable, and any such partitioning of the blocks is said to be a resolution. Any set of $(v-1)/k$ pairwise disjoint blocks together with a singleton consisting of the only element not in one of the blocks is called a parallel class. Any resolution of a design yields v parallel classes. We denote by RPD$(v, k, 1)$ the class of all resolvable perfect cyclic designs with parameters v, k, and 1. Associated with any resolvable perfect cyclic design is an orthogonal array with $k+1$ columns and v rows with an interesting conjugacy property. Also a design in the class RPD$(v, k, 1)$ is constructed for all sufficiently large v with $v \equiv 1 \bmod k$.

1. INTRODUCTION, DEFINITIONS, AND REQUIRED THEOREMS

This paper is concerned with a certain type of design which is interesting in itself and which is useful for the study of a certain class of orthogonal array. We require several definitions. If S is a set of positive integers and T is a subset of S such that $S - T$ is finite, we say that T is an asymptotic subset of S. If K is a finite set of positive integers, we define $\alpha(K)$ as the g.c.d. $\{k(k-1) \mid k \in K\}$ and $\beta(K)$ as the g.c.d. $\{k-1 \mid k \in K\}$. A set of k distinct elements $[a_1, a_2, \ldots, a_k]$ is said to be cyclically ordered by $a_1 < a_2 < a_3 \cdots < a_k < a_1$. The pair a_i, a_{i+t} ($i + t$ taken mod k) are said to be t apart. The set $[a_1, a_2, \ldots, a_k]$ is called a k-cyclic set. A perfect k-cyclic design of index λ is defined as a pair (P, B) where P is a set, B is a collection of k-cyclic sets made up of elements of P, and such that any ordered pair u, v of elements of P appear t apart in exactly λ of the k-cyclic sets for $t = 1, 2, 3, \ldots, k-1$. The k-cyclic sets of B are also referred to as blocks when no

0097-3165/80/050142–09$02.00/0

ambiguity arises. If $v = |P|$, v is called the order of the design and a simple count shows that $|B| = \lambda(v(v-1)/k)$. The integers v, k, and λ are called the parameters of the design and any design with these parameters is said to belong to the class PD(v, k, λ). In what follows we restrict ourselves to designs with $\lambda = 1$ (i.e., of index 1). In a design of index 1, with $v \equiv 1 \bmod k$ we define the notion of resolvability. Suppose the blocks can be partitioned into v sets each containing $(v-1)/k$ blocks which are pairwise disjoint (as sets). In this case, we say the design is resolvable and any such partition is called a resolution. Any set of $(v-1)/k$ pairwise disjoint blocks together with a singleton consisting of the only element of P which is not in one of the blocks is called a parallel class. Any resolution of a design yields v parallel classes. We denote by RPD$(v, k, 1)$ the class of all resolvable perfect k-cyclic designs with parameters v, k, 1. In our constructions we also need the notion of a pairwise balanced design. Such a design is a triple (P, B, K) where P is a finite set, B is a collection of subsets of P called blocks, and K is a set of positive integers where the cardinality of each block of B belongs to K and where every pair of distinct elements of P belong to exactly one block. Here, $v = |P|$ is called the order of the design. An important theorem of Wilson [6] states that such a design exists for an asymptotic subset of the integers v which satisfy the two congruences $v(v-1) \equiv 0 \bmod \alpha(K)$, $v - 1 \equiv 0 \bmod \beta(K)$. Next we need some notions taken from universal algebra. For our purposes a universal algebra consists of a pair (A, O) where A is a set and O is a finite set of finitary operators where an n-ary operator is a mapping of $A^n \to A$. An n-ary operator f is called idempotent if for all x, $f(x, x, \ldots, x) = x$. A quasi-variety of universal algebras is a collection of such algebras each with the "same" operators and each satisfying a set of statements of the form "$\forall(x, y, z, \ldots)$ if $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2, \ldots$, and $\alpha_r = \beta_r$ then $\alpha = \beta$" where $\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha, \beta_1, \beta_2, \ldots, \beta_r, \beta$ are properly formed expressions in the variables x, y, $z, \ldots$ If all the statements are of the form "$\forall(x, y, \ldots)$ $\alpha = \beta$" the quasi-variety is called a variety. The spectrum of a quasi-variety is the set of all integers v for which there is an algebra with v elements in the quasi-variety. From the combinatorial point of view the main uses of quasi-varieties comes from the fact that subalgebras and direct products of algebras in the quasi-variety also lie in the quasi-variety. There is one important other use which comes from the following almost trivial observation. Suppose we have a quasi-variety of idempotent algebras based on binary operators and on two variable statements. Suppose further that there are algebras of orders $k_1, k_2, \ldots, k_t$ within the quasi-variety and that there is a pairwise balanced block design of index one which is of order v and with block sizes in $K = \{k_1, k_2, \ldots, k_t\}$. Then v is in the spectrum of the quasi-variety. It follows from Wilson's theorem that the quasi-variety has a spectrum which contains an asymptotic subset of the set of all v satisfying $v(v-1) \equiv 0 \bmod \alpha(K)$, $v - 1 \equiv 0 \bmod \beta(K)$. The main types of

universal algebra used in combinatorics are the groupoid which is an algebra with a single binary operator and the quasi-group which is a groupoid with the added condition that in an equation $x * y = z$ ($*$ is the groupoid operator) any two of x, y, and z uniquely determine the third. By introducing two inverse operators and appropriate identities, quasi-groups may be looked upon as a variety of algebras based on two-variable identities in three binary operators.

2. The Algebraic and Combinatorial Constructions

First we define a quasi-variety with the property that a resolvable perfect k-cyclic design together with a specific resolution can be constructed from the algebra, and conversely, from such a design and resolution the algebra can be recovered.

Let $*$ be a binary operator. Put $V_0(x, y) = x$, $V_1(x, y) = x * y$, $V_2(x, y) = (x * y) * y$, and recursively $V_n(x, y) = V_{n-1}(x, y) * y$ for $n = 2, 3, 4, 5,...$ Now define a quasi-variety of quasi-groups by means of the statements:

(1) For all x, y, $V_k(x, y) = x$.

(2) For all x, y if $V_n(x, y) = x$, then $x = y$ for $n = 1, 2, 3,..., k - 1$.

(3) For all x, y, u, if $V_n(x, y) = V_n(x, u)$, then $y = u$ for $n = 1, 2,..., k - 1$.

We denote this quasi-group quasi-variety by Q_k. Three things may be noted. First, statement (2) implies that the quasi-variety is idempotent. Second, in any finite algebra in Q_k statement (3) implies that given a and b and n an integer less than k, the equation $V_n(a, x) = b$ uniquely determines x. Finally, in spite of the fact that statement (3) involves three variables, all the remarks about two-variable quasi-varieties made in the introduction are valid for Q_k.

THEOREM 1. *Let A be an algebra in Q_k such that $|A| = v$. Then $v \equiv 1 \bmod k$ and there is a design in the class* RPD(v, k, 1).

Proof. For each $y \in A$ we set up a parallel class with y as singleton as follows. Let $x \neq y$. Take as a k-cyclic block the block $[x, V_1(x, y), V_2(x, y),..., V_{k-1}(x, y)]$. Note that conditions (1)–(3) assure that no two elements in this block are equal and the block is uniquely determined by any one of its elements. If the elements of A are not used up, take an element u which has not yet appeared and form the block $[u, V_1(u, y),..., V_{k-1}(u, y)]$. This block is setwise disjoint from y and the previous block. The process is continued until all elements of A are used. Hence $v = |A| \equiv 1 \bmod k$. For each element of A form the corresponding parallel class. The set of

$(v(v-1))/k$ blocks so formed constitute the blocks of the design. We need only verify that any ordered pair u, v of elements of A lie r apart in exactly one block. This follows from the fact that the equation $V_r(u, x) = v$ determines x uniquely and in the parallel class with x as singleton, u and v are r apart in the block

$$[u, V_1(u, x),..., V_r(u, x),..., V_{k-1}(u, x)]$$

THEOREM 2. *Suppose there is a resolvable k-cyclic design on v elements and a specific resolution. Then one can construct a quasi-group in Q_k associated with the resolution.*

Proof. Let u and v be two elements of the design. Consider the unique block containing u in the parallel class with singleton v. If w follows u in this block, define $u * v$ by putting $u * v = w$. A simple check verifies that the algebra is a quasi-group in Q_k.

Remark. Different resolutions of the same design yield different quasi-groups which may not be isomorphic.

THEOREM 3. *If q is a prime power such that $q \equiv 1 \bmod k$, there is a quasi-group of order q in Q_k.*

Proof. Take as our set of elements the elements of the galois field GF(q). The multiplicative group of GF(q) is cyclic of order $q-1$. Since $k \mid q-1$ there is an element λ in GF(q) of order k. Define for any pair of elements x and y in GF(q) the product $x * y = \lambda x + (1-\lambda)y$. Inductively, it follows that $V_r(x, y) = \lambda^r x + (1-\lambda^r)y$. From this, statements (1)–(3) concerning quasi-groups in Q_k follow immediately.

THEOREM 4. *A k-cyclic design of order v exists for an asymptotic subset of all $v \equiv 1 \bmod k$.*

Proof. We distinguish two cases.

Case 1. k is even. Consider the arithmetic progression $\{1-k+mk(1+k) \mid m = 1, 2, 3,...\}$. Since $k-1$ is odd, g.c.d. $(1-k, k(1+k)) =$ g.c.d.$(1-k, (k+2)(k-1)+2) =$ g.c.d.$(1-k, 2) = 1$. Hence, by Dirichlet's theorem there is an m for which $p = 1-k+mk(1+k)$ is prime. Again, for the arithmetic progression $\{1+k+u\ (km+mk^2-k) \mid u = 1, 2, 3,...\}$ the g.c.d. $(1+k, k(m+mk-1)) =$ g.c.d.$(1+k, m+mk-1) =$ g.c.d.$(1+k, -1) = 1$. Hence, there is a u for which $q = 1+k+u(km+mk^2-k)$ is a prime. Since both $p \equiv 1 \bmod k$ and $q \equiv 1 \bmod k$, there are quasi-groups of orders p and q in Q_k.

We now choose a third prime $r \equiv 1 \bmod k$ as follows. Since g.c.d. $(k, p) = 1$, then by the Chinese remainder theorem there is an integer s such that $s \equiv 1 \bmod k$ and $s \equiv 2 \bmod p$. This implies that g.c.d. $(s, kp) = 1$ so that the arithmetic progression $\{s + fkp \mid f = 1, 2, 3, \ldots\}$ contains primes. Take f so that $r = s + fkp$ is prime. Then $r \equiv 1 \bmod k$ and $r \equiv 2 \bmod p$. Now there is an algebra of order r in Q_k. Let $K = \{p, q, r\}$. Then $\beta(K) =$ g.c.d. $(p-1, q-1, r-1)$. Since k is a common divisor of $p-1$, $q-1$, $r-1$, $k \mid \beta(K)$. But g.c.d. $(p-1, q-1) =$ g.c.d.$(-k + mk(1+k), k + u(km + mk^2 - k)) =$ k(g.c.d.$(-1 + m(1+k), 1 + u(-1 + m(1+k))) =$ k(g.c.d.$(-1 + m(1+k), 1)) = k$. Hence $\beta(K) = k$. Also $\alpha(K) =$ g.c.d.$(p(p-1), q(q-1), r(r-1))$. First compute g.c.d.$(p(p-1), q(q-1))$. Since p and q are primes with $q > p$ and g.c.d.$(p-1, q-1) = k$, then g.c.d.$(p(p-1), q(q-1)) = k$ if $p \nmid q-1$ and equals kp if $p \mid q-1$. But p is prime to both r and $r-1$ and hence $\alpha(K) = k$. Hence the spectrum of Q_k contains an asymptotic subset of the v which satisfy $v(v-1) \equiv 0 \bmod k$ and $v \equiv 1 \bmod k$, the first of these congruences being redundant since it is implied by the second. Combining this result with that of Theorem 1 it follows that the spectrum of Q_k is an asymptotic subset of the v satisfying $v \equiv 1 \bmod k$.

Case 2. k is odd. Replace k by $2k$ in computing the primes p, q, r. Since $p \equiv 1 \bmod k$, $q \equiv 1 \bmod k$, and $r \equiv 1 \bmod k$, the numbers p, q, r are in the spectrum of Q_k. Also g.c.d.$(p-1, q-1, r-1) = 2k$ and g.c.d.$(p(p-1), q(q-1), r(r-1)) = 2k$. Since k is odd, $2^{\phi(k)} \equiv 1 \bmod k$ so that the prime power $2^{\phi(k)}$ is in the spectrum of Q_k. Taking $K = \{p, q, r, 2^{\phi(k)}\}$ it follows that $\alpha(K) = 2k$, $\beta(K) = k$ (since $2^{\phi(k)} - 1$ is odd). Hence, the spectrum contains an asymptotic subset of the v which satisfy $v(v-1) \equiv 0 \bmod 2k$, $v \equiv 1 \bmod k$. Again the first congruence is redundant since k is odd.

3. Application to Orthogonal Arrays

An orthogonal array OA(c, n^2) is a rectangular array with n^2 rows and c columns whose entries come from an n-set S, and such that for any pair of columns every ordered pair of elements of S (not necessarily distinct) appear in the same row exactly once. From an OA(c, n^2) one constructs a set of $c-2$ pairwise orthogonal latin squares by using the first two columns to determine the row and column indices and the corresponding entry in the $(r+2)$nd column is the entry in the rth latin square. From the point of view of constructing orthogonal latin squares we consider two orthogonal arrays to be equivalent if one is obtained from the second by permuting its rows. In general, if we permute the columns of an OA(c, n^2), we get a different set of row vectors. Let us define a conjugacy of an orthogonal array as a permuta-

tion of its columns the effect of which is to permute its rows. Such conjugacies form a group and it is an interesting question to determine which groups are conjugacy groups of orthogonal arrays and for a given group to determine the orthogonal array spectrum, i.e., determine the set of n for which an $OA(c, n^2)$ exists with the given group as its conjugacy group. Lindner and Mendelsohn [4] have obtained some results on the problem for $c = 4$. We now give a construction of an $OA(k+1, n^2)$ from a resolvable perfect k-cyclic design of order n.

THEOREM 5. *To each resolvable k-cyclic design of order n, $n \equiv 1 \bmod k$, and with each resolution there is an associated orthogonal array $OA(k+1, n^2)$ which admits as conjugacies the cyclic permutations of its first k columns.*

Proof. Suppose the design is based on the symbols 1, 2,..., n. Form the array with $k+1$ columns as follows. Take the first n rows to be

$$\begin{array}{l} 1\ 1\ 1\ \ldots\ 1 \\ 2\ 2\ 2\ \ldots\ 2 \\ \vdots \\ n\ n\ n\ \ldots\ n. \end{array}$$

The first k columns of the array is completed by taking each k-cyclic block and use it to fill k rows of the array by writing down all its cyclic permutations. Finally, fill in the last column by entering in each row the singleton which belongs to the parallel class which contains the block which already appears in that row. It is immediately verified that the n^2 by $k+1$ array is an $OA(k+1, n^2)$ which admits as conjugacies the cyclic permutations of the first k columns.

COROLLARY. *The spectrum of $OA(k+1, n^2)$ which admit as a conjugacy a cyclic permutation of k of its columns contains an asymptotic subset of the set of $n \equiv 1 \bmod k$.*

EXAMPLE. Let $k = 3$, $n = 7$. The following is a resolution of a design of order 7 with block size 3.

1	2	3	4	5	6	7
2 3 5	1 7 5	1 6 2	1 5 6	1 4 3	1 3 7	1 2 4
4 7 6	3 4 6	4 5 7	2 7 3	2 6 7	2 5 4	3 6 5

yielding the array OA(4, 49) given by the table

1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
2	3	5	1
3	5	2	1
5	2	3	1
4	7	6	1
6	4	7	1
7	6	4	1
1	7	5	2
5	1	7	2
7	5	1	2
3	4	6	2
6	3	4	2
4	6	3	2
1	6	2	3
2	1	6	3
6	2	1	3
4	5	7	3
7	4	5	3
5	7	4	3
1	5	6	4
6	1	5	4
5	6	1	4
2	7	3	4
3	2	7	4
7	3	2	4
1	4	3	5
3	1	4	5
4	3	1	5
2	6	7	5
7	2	6	5
6	7	2	5
1	3	7	6
7	1	3	6
3	7	1	6
2	5	4	6

4 2 5 6
5 4 2 6
1 2 4 7
4 1 2 7
2 4 1 7
3 6 5 7
5 3 6 7
6 5 3 7

4. Resolvable Perfect 3-Cyclic Designs

For the case $k = 3$, the results now known are complete with respect to the spectrum and are given in what follows: For $n = 10$, the set of all systems and their resolutions has been obtained by Ganter,[1] Mathon, and Rosa [2]. These have yielded a plethora of pairs of orthogonal latin squares of order 10, but none of these are extendable to a pairwise orthogonal triple.

The quasi-variety Q_3 is simply the variety of quasi-groups satisfying the identities

$$((x * y) * y) * y = x$$

and

$$x * x = x.$$

By Theorem 3, the spectrum of Q_3 contains the integers 4, 7, and 19, and by Ganter, Mathon, and Rosa [2], also contains 10. Hanani [3] has shown that there is a pairwise balanced design with block size 4, for all $v \equiv 1$ or 4 mod 12 and Brouwer [1] has shown that a pairwise balanced design with one block of size 7 and the remaining blocks of size 4 exists for all $v \equiv 7$ or 10 mod 12 except $v = 10$ or 19. Combining this information we obtain that the spectrum of Q_3 contains all $v \equiv 1 \bmod 3$.

5. Further Remarks

In [5], Mendelsohn has obtained perfect k-cyclic designs for certain values of v where $v \not\equiv 1 \bmod k$. In particular for k an odd prime, designs with $v \equiv 0 \bmod k$ have been found. The methods used are the same as those used in this paper using a different but related quasi-variety. However, questions of resolvability have not been solved in these cases.

[1] These authors call a perfect 3-cyclic design a Mendelsohn triple system.

REFERENCES

1. A. E. BROUWER, Optimal Packings of K_4's into a K_n, *J. Combinatorial Theory Ser. A* **26** (1979), 278–297.
2. B. GANTER, R. MATHON, AND A. ROSA, A complete census of (10, 3, 2)-block designs and of Mendelsohn triple systems of order ten, Proc. Seventh Manitoba Conf. Numerical Math. and Computing, 1977, pp. 383–398.
3. H. HANANI, Balanced incomplete block designs and related designs, *Discrete Math.* **11** (1975), 255–369.
4. C. C. LINDNER AND E. MENDELSOHN, On the conjugates of an $n^2 \times 4$ orthogonal array, *Discrete Math.* **20** (1977), 123–132.
5. N. S. MENDELSOHN, Perfect cyclic designs, *Discrete Math.* **20** (1977), 63–68.
6. R. M. WILSON, An existence theory for pairwise balanced designs III, *J. Combinatorial Theory* **18** (1975), 71–79.